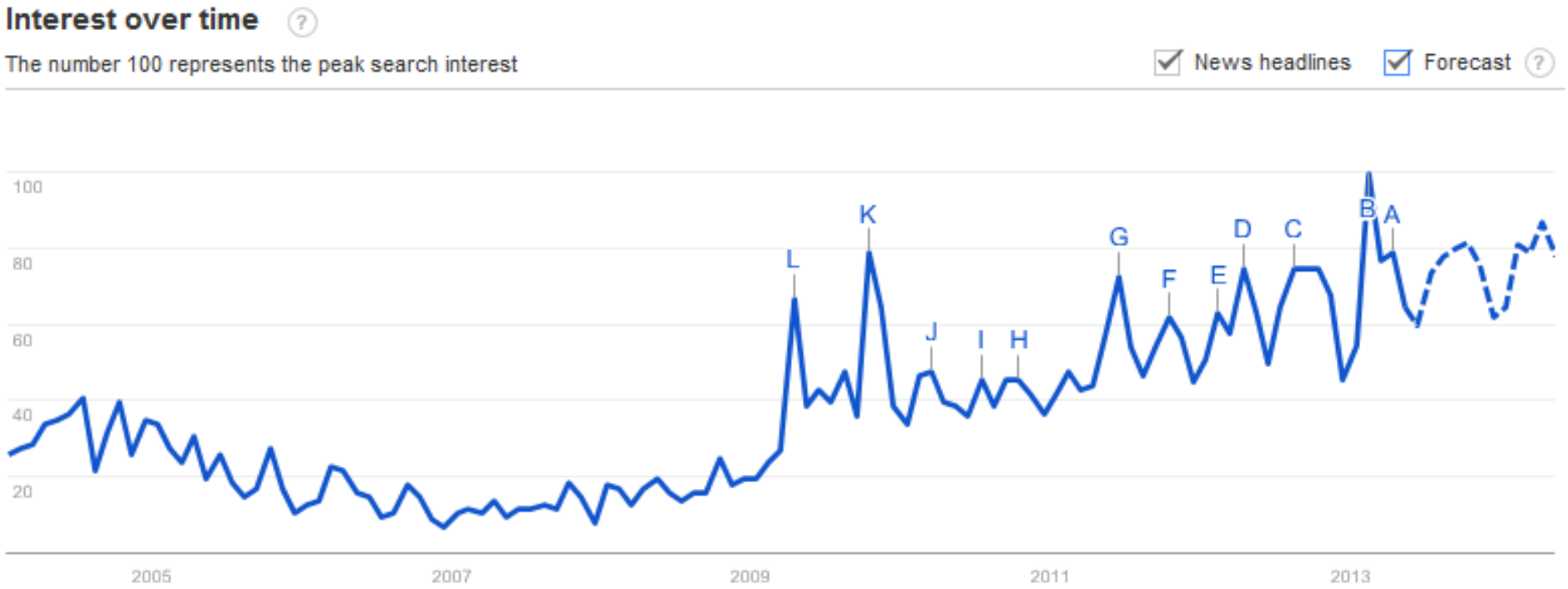
8 August 2013

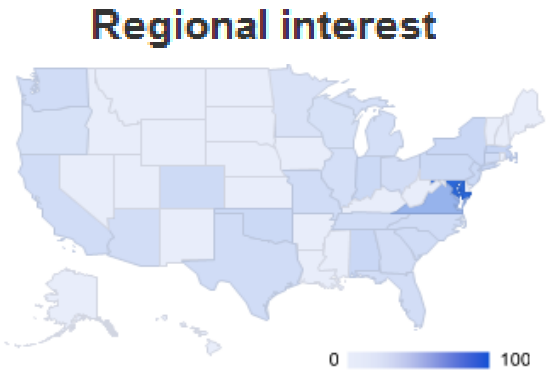
Homeland Security

Homeland Security Perspectives:
Building and Evaluating Cyber Resilience

Bradford Willke, CISSP
Cyber Security Advisor, Mid-Atlantic Region
Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Google Trends: “cyber security”



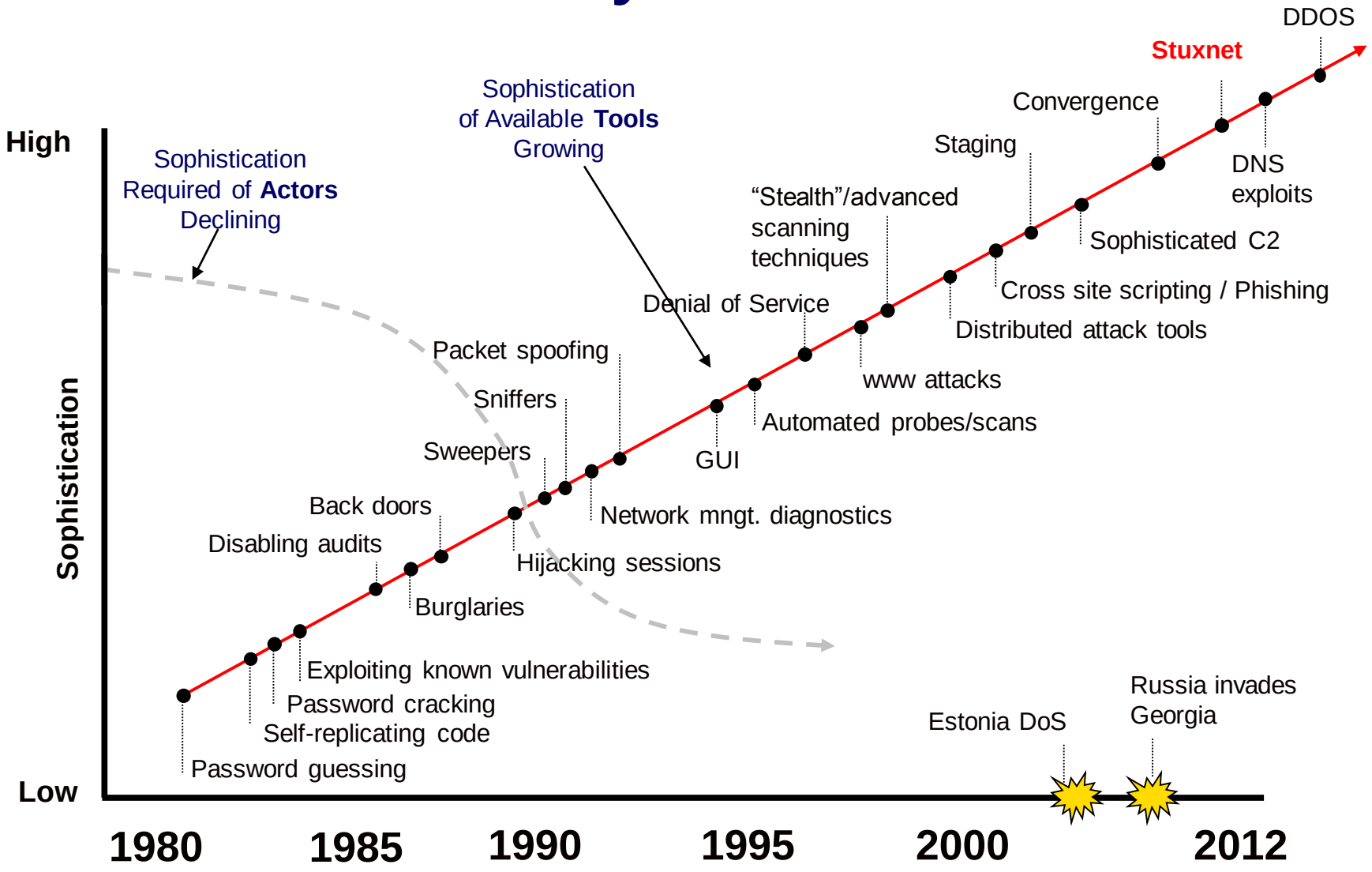


Homeland Security

CYBER THREAT TRENDS AND SPECIFIC ATTACKS

Homeland Security

Growth of Cyber Threats



Homeland Security

Cyber Threat: Human Threats

Who is behind these intentional threats?

- Insider Threat
  - Insiders have a unique advantage due to access/trust
  - They can be motivated by revenge, organizational disputes, personal problems, boredom, curiosity, or to "prove a point"
- Malware Authors
  - Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware
- Phishers
  - Individuals, or small groups who attempt to steal identities or information for monetary gain
- Spammers
  - Individuals or organizations who distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations
- Terrorists
  - Cyber attacks have the potential to cripple unsecured infrastructures
  - Cyber-linkages between sectors raise the risk of cascading failure

Homeland Security

2012: Targeted cyber attack on pipelines

- **23 targeted pipeline** operators (December 2011 – June 2012)
- **9 confirmed**, 3 near misses, 11 pending
- Adversary is targeting industrial control systems information
  - Document searches: “SCAD*”
    - Personnel Lists
    - Usernames/Passwords
    - Dial-Up access information
    - System manuals
  - Exfiltrated ICS access credentials
- The data exfiltrated could provide an adversary with the capability to access US ONG ICS including performing unauthorized operations

Homeland Security

What was taken?

- All_gate_meter.xls
- **<station>_SCADA 8-23-2002.vsd**
- Contact List Gas Scada.xls
- <redacted>_Area_RTUs.xls
- **Dial Up #### Vector Lists.xls**
- SCADA_Server_UsersGuide.pdf
- Gas Control Numbers.xls
- Gas SCADA Profiles Defined 10-22-03.xls
- Gas-Control Asset list.xls
- **<station> Dialup.xls**
- PASS1.xls
- <station> datapoints for log.xls
- RTU point list.xls
- **RTU SITES.xls**
- SCADA Division Options.ppt
- SCADA HARDWARE UPGRADE.ppt
- SCADA Sites.xls
- Scada Users Manual.zip
- **SCADA_logons.doc**
- **Security.zip**
- Standard Colors & Symbols.xls
- Station Control Testing Procedures.ppt
- **DIALUP.DOC**
- DISPLAYS.DOC
- <station> Comm Card Converter pinout.pdf
- Comm Ports for Airlink.pdf
- D-Sub to RJ45 Modular Adapters.pdf
- **SCADA Personnel.html**

Homeland Security

Shamoon Attack Against Aramco

- Saudi Aramco is based in Saudi Arabia, but also maintains offices in the United States, was attacked on August 15th
- “The Cutting Sword of Justice” is claiming responsibility
- Saudi Aramco reports that approximately 30,000 machines were affected
- Saudi Aramco maintains that their oil production was not impacted as a result of this attack.

Homeland Security

Shamoon Attack Against Aramco

- Highly destructive, renders infected systems useless after stealing information
  - Overwrites Master Boot Record (MBR), partition tables, and most files with random data.
  - Overwritten data is non-recoverable
  - Hard drives were overwritten with an image of a burning American flag
- Evidence exists that some variants are not detected by major AV companies
- Similar attacks in US could have significant impact on US Companies

Homeland Security

RasGas Networks Impacted by Shamoon

- August 2012: Qatar's RasGas discovered a virus on their enterprise network
- Email servers and website services were disrupted
- According to open-source, no operational systems, production, or shipments were impacted
- Very similar impacts experienced by Saudi Aramco
  - **Not detected by AV**
  - Payload change
  - Initial compromise early May
  - Highly targeted

RasGas

Homeland Security

Key Resilience Domains

When Resilience Fails – NE Power Outage – August 14, 2003

AM	**Asset Management** *identify, document, and manage assets during their life cycle*	IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	SCM	**Service Continuity Management** *ensure the continuity of essential IT operations in disruption occurs*
RISK	**Risk Management** *identify, analyze, and mitigate risks to critical service and IT assets*	EXD	**External Dependencies Management** *establish processes to manage an appropriate level of IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge of people*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

Homeland Security

DHS CYBER COORDINATION AND INCIDENT RESPONSE

Homeland Security

Office of Cybersecurity and Communications

MISSION:

To enhance the security, resilience, and reliability of the Nation's cyber and communications infrastructure.

Capabilities:

- CS&C works collaboratively with public, private, and international entities to secure, assess, and mitigate cyber risk; and prepare for, prevent, and respond to cyber incidents.
- CS&C leads efforts to protect the federal "**.gov**" domain of civilian government networks and to collaborate with the private sector—the "**.com**" domain—to increase the security of critical networks.
- Build and maintain a world-class organization to advance the Nation's cybersecurity preparedness and raise awareness across the Nation on cybersecurity
- Sector-Specific Agency for the Communications and Information Technology (IT) sectors, CS&C coordinates national-level reporting that is consistent with the National Response Framework (NRF).

Homeland Security

NCCIC in Brief

The mission of the **National Cybersecurity and Communications Center (NCCIC)** is to serve as a national center for reporting of and mitigating communications and cybersecurity incidents.

http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

Responsibilities include:

- Provide alerts, warnings, common operating picture on cyber and communications incidents in real time to virtual and on-site partners
- Work 24X7 with partners to mitigate incidents:
  - On-site partners include the Department of Defense, Federal Bureau of Investigation, Secret Service, Information Sharing and Analysis Centers (ISACs) and DHS components such as Office of Industry and Analysis
  - Public and private sector partners share and receive information subject to information sharing protocols

Homeland Security

US-CERT: Response & Assistance

- Activities are based on the nature and severity of the incident, and focus on tracking impacted parties' progress toward resolving the issue
- Dedicated teams ensure appropriate and accurate technical assistance is provided with the right level of subject matter expertise, including:
  - ✓ Digital Media and Malware Analysis
  - ✓ Defensive Analysis
  - ✓ Mitigation Strategy Development
  - ✓ Threat / Attack Vector Analysis
  - ✓ Vendor Analysis Coordination

- Deployable teams can provide specialized subject matter expertise required to mitigate an incident or prevent an event from escalating

Homeland Security

ICS-CERT

Provide operational support for critical infrastructure stakeholders to respond and defend against emerging cyber threats

Situational Awareness

Observe, identify, acquire, or receive relevant ICS information

Incident Response

Provide on-site assistance and off-site analysis to bridge information gap

Technical Analysis

Perform digital media analysis for malware and consequences

Vulnerability Coordination

Coordinate and monitor for vulnerabilities in ICS systems

Benefits to the ICS and Critical Infrastructure Community

- Awareness of emerging issues and threats
- State of the art analysis capabilities specific to ICS
- Incident response support for recovery and future defense
- Established partnership for immediate support and guidance
- ICS-CERT collaboration with other agencies and partners

Homeland Security

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Subject Matter Experts in Industrial Control Systems (ICS)

- Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Distributed Control Systems (DCS), Remote Terminal Units (RTUs), Human Machine Interfaces (HMIs), Programmable Logic Controllers (PLCs)

Unique Awareness of Emerging Issues and Threats to Control Systems and Vendor Products

State of the Art Analysis Capabilities Specific to ICS that enable –

- Malware and Embedded Systems Analysis
- Patch Testing
- Consequence Analysis

Incident Response Support for ICS-Related Response, Recovery and Future Defense Efforts

ICS-CERT Quickly Reacting to Threats – FY12

- Received and responded to 198 cyber incidents
- Published 332 information products alerting the community to vulnerabilities and threats

ICS-CERT Proactively Assisting Others – FY12

- Tracked 171 unique vulnerabilities affecting ICS products and coordinated the vulnerabilities with 55 different vendors
- Provided 56 in-person training sessions
- Analyzed over 50 malware samples and malicious files, 20 emails, and 38 hard drive images for the ICS/SCADA environment

Homeland Security

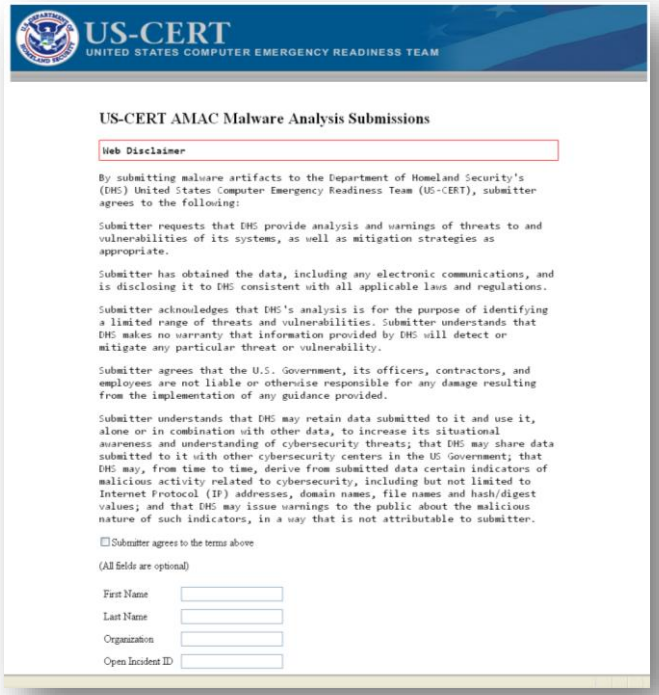
Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870

Malware Submission Process:

- Please send all submissions to AMAC at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission: https://malware.us-cert.gov


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT AMAC Malware Analysis Submissions

Web Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknouledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

☐ Submitter agrees to the terms above

(All fields are optional)

First Name

Last Name

Organization

Open Incident ID

Protection of Information

Traffic-Light Protocol (TLP): Originator-controlled classification system developed to encourage greater sharing of sensitive (but unclassified) information with external entities.

When should it be used?	TLP Color	How may it be shared?
Sources may use TLP: **RED** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting or conversation in which it is originally disclosed.
Sources may use TLP: **AMBER** when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER	Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.
Sources may use TLP: **GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: **WHITE** when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Homeland Security

State & Local Programs / MS-ISAC

Improve cyber threat coordination

Work to jointly establish a unified information sharing process:

- Coordinate suspicious activity reports
- Coordinate incident management, including:
  - Requests for technical assistance
  - Requests for non-technical incident handling
  - Law enforcement assistance
  - Incident notification and reporting
- Threat analysis and/or threat product redistribution

Participate in state and local cyber steering committees and working groups

Homeland Security

Cyber Partnership Examples

- Area Maritime Security Committee: Cyber Sub-Committee (Pittsburgh)
- Philadelphia FBI Field Office – Computer Intrusion Threat Analysis System (CITAS) Project
- ICS Security Working Group (Pittsburgh)
- Pittsburgh, Buffalo, Philadelphia, etc, FBI Cyber Squads

Homeland Security

Area Maritime Security Committee: Cyber Sub-Committee

- DHS, USCG, CIKR, and Business Partnership
- Committee Premises:
  - Incident response and continuity of operations still need work
  - Partners need credible planning templates and test-able scenarios
  - A SME database for cyber responders is useful and needed
  - Organizations need a “411” system for information on where to voluntarily report, request technical assistance, request non-technical incident handling, request law enforcement responses, to cyber incidents
  - Organizations would benefit from a local emergency management, “911-like,” function that mobilizes regional and local cyber responses – and creates a regional common operating picture

Homeland Security

CITAS Overview

- FBI, InfraGard, and DCIS Project (Philadelphia-Area)
- Project Premises:
  - Create a honeynet / honeypot environment in the corporate DMZ
  - Create “look and feel” but non-referencing system(s) as targets
  - Take “what you know” and use it as a filter
  - Find the intermediary victims and unique signatures of adversaries (not just attacking systems)
- Project Successes:
  - Notification to those already compromised
  - Active investigations of real adversaries
  - Improve signatures of known attacks

Homeland Security

ICS Security Working Group

- DHS, FBI, NCFTA, and Industry Partnership
- Working Group Premises:
  - Exchange credible, relevant cyber security issues, attacks, and trends
  - Share lessons-learned from specific “deployments” of ICS
  - Demonstrate a security model involving defense-in-depth and layer defenses
  - Deliver challenge-based requirements to federal, state, and local partners

Homeland Security

DHS ICS Informational Products and Services

ADVISORIES, REPORTS, ETC

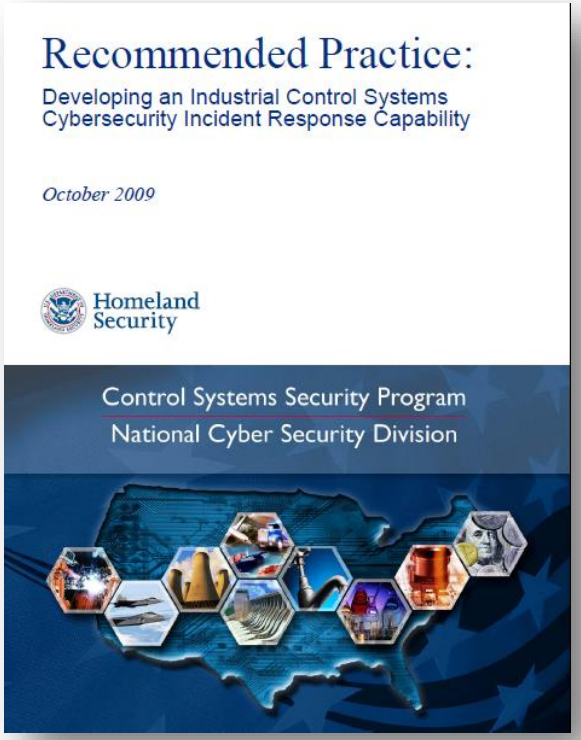
HTTPS://ICS-CERT.US-CERT.GOV/

Homeland Security

DHS Recommended Practices

Homeland Security

DHS Recommended Practices



Homeland Security

ICS-CERT Special Reports

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

CERT analyzed the malware and its impacts to control systems in coordination with various government agencies, law enforcement, industry, and other organizations such as Symantec, Microsoft, CERT Bund, Siemens, and various sector ISACs (i.e., Energy, Chemical, Nuclear, Dams, Water, Transportation). ICS-CERT issued advisories with multiple updates to provide mitigation information to critical infrastructure asset owners and operators. ICS-CERT also conducted an onsite incident response deployment to a manufacturing facility infected with the Stuxnet malware and helped the organization identify all infected systems and eradicate the malware from their control system network (see page 8, "Onsite Incident Response Activities" for more details).

2011

REPORTED INCIDENTS

In 2011, ICS-CERT received 198 reports of incidents. Of those 198, seven resulted in the deployment of onsite incident response teams. An additional 21 incidents involved analysis efforts by the AAL to identify malware and techniques used by the threat actors. Figure 4 displays the sector distribution for all incidents reported in 2011. Incidents specific to the Water Sector, when added to those that impacted multiple sectors, accounted for over half of the incidents due to a large number of Internet facing control system devices reported by independent researchers.

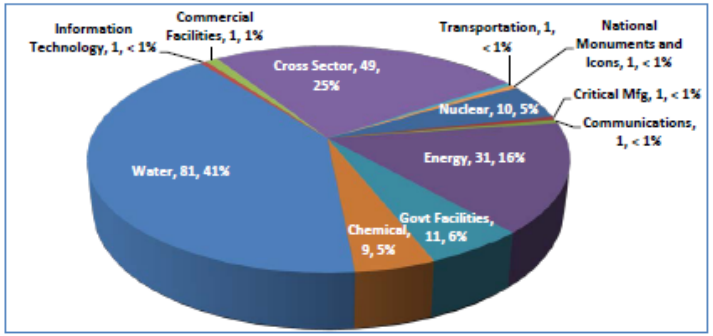
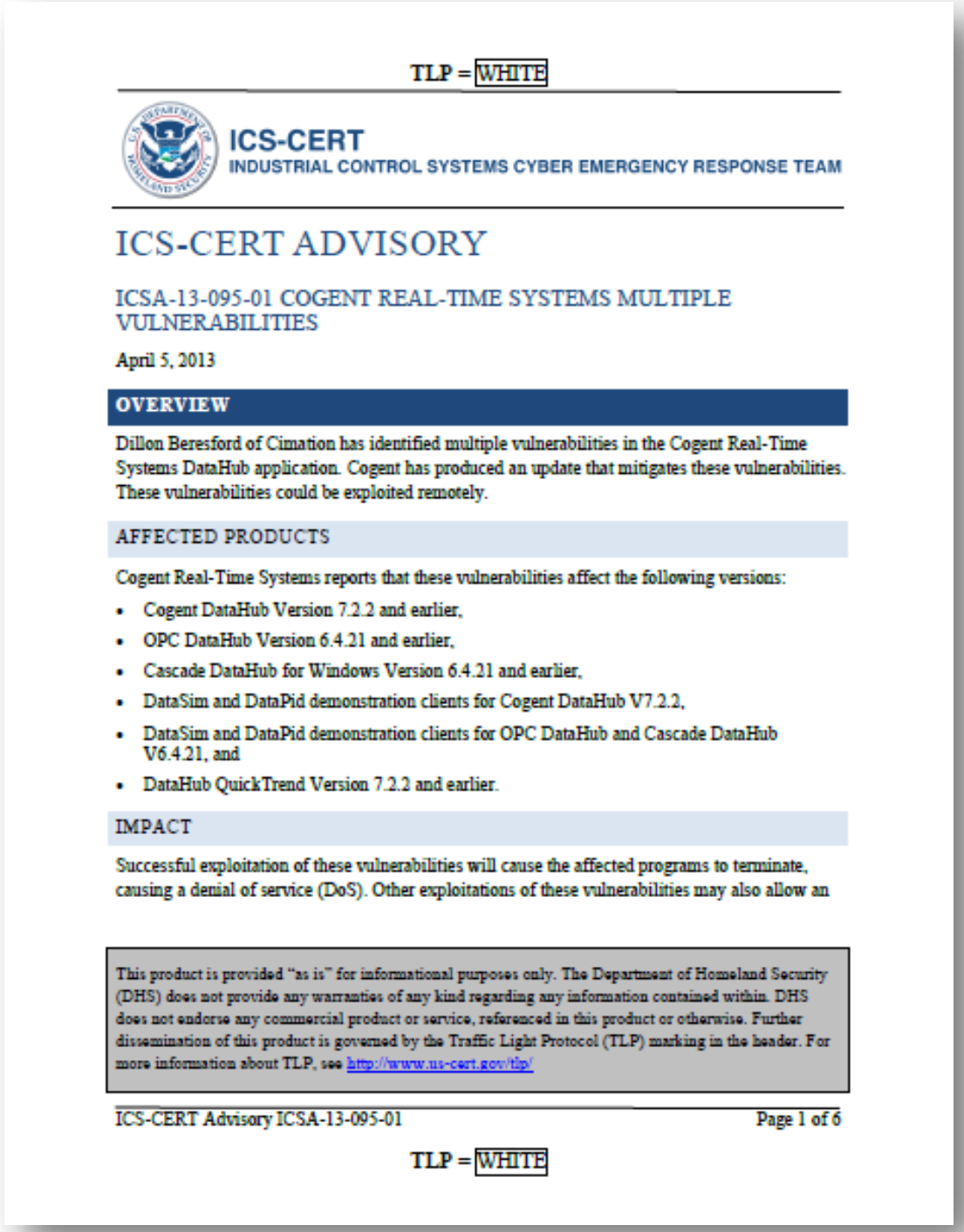


Figure 4. Incident reports by sector (2011).

Many of these Internet facing control systems employed a remote access platform from the same vendor, configured with an unsecure authentication mechanism. ICS-CERT coordinated with the vendor to mitigate the authentication vulnerability and also took on the task of identifying and notifying the affected asset owners. ICS-CERT provided them with details of the risks associated with weak boundary

Homeland Security

Industrial Control System Advisories



TLP = WHITE

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-095-01 COGENT REAL-TIME SYSTEMS MULTIPLE VULNERABILITIES

April 5, 2013

OVERVIEW

Dillon Beresford of Cimation has identified multiple vulnerabilities in the Cogent Real-Time Systems DataHub application. Cogent has produced an update that mitigates these vulnerabilities. These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

Cogent Real-Time Systems reports that these vulnerabilities affect the following versions:

- Cogent DataHub Version 7.2.2 and earlier,
- OPC DataHub Version 6.4.21 and earlier,
- Cascade DataHub for Windows Version 6.4.21 and earlier,
- DataSim and DataPid demonstration clients for Cogent DataHub V7.2.2,
- DataSim and DataPid demonstration clients for OPC DataHub and Cascade DataHub V6.4.21, and
- DataHub QuickTrend Version 7.2.2 and earlier.

IMPACT

Successful exploitation of these vulnerabilities will cause the affected programs to terminate, causing a denial of service (DoS). Other exploitations of these vulnerabilities may also allow an

TLP = WHITE

Homeland Security

ICS-CERT Training – 5 Day Course

- **Next "open" session:** November 4-8, 2013 at Idaho Falls, ID
- **Description:** Hands-on training in discovering who and what is on the network, identifying vulnerabilities, learning how those vulnerabilities may be exploited, and learning defensive and mitigation strategies for ICS
  - Includes a Red Team / Blue Team exercise that takes place within an actual control systems environment
- **Who Should Attend?** Members of the ICS community associated with IT and process control network operations and security, operations or management of critical infrastructure (CI) assets and facilities as well as those who provide CI components and software development
- **Cost to Attend:** None
  - However, travel expenses to and from and accommodations at Idaho Falls are the responsibility of each participant
- **For more information/registration:** https://secure.inl.gov/icsadv1113/
- *For a list of scheduled training: http://ics-cert.us-cert.gov/cscalendar.html*

Homeland Security

Cyber Security Advisor Initiative

Roles and Responsibilities

- Assist in the identification of cyber systems, networks, and infrastructure supporting CIKR assets and be knowledgeable of corresponding interdependencies in their region
- Coordinate and lead cyber security evaluations of critical infrastructure within the region represented
- Raise awareness of CS&C activities
- Function as the National Cyber Security Division representative to State and local emergency operations centers (EOCs) and State and local fusion centers
- Establish working relationship and rapport with State and local area CISOs in the region represented
- Coordinate with Federal personnel within region to integrate cyber security response and assessment perspectives (i.e., with PSAs, FEMA, Federal LE, etc)
- Other duties as assigned to align with evolving CS&C goals and objectives

Homeland Security

Evolving Federal Policy

PRESIDENTIAL POLICY DIRECTIVE 21 (PPD-21) & EXECUTIVE ORDER 13636 (EO)

Homeland Security

Presidential Policy Directive - 21

Three Strategic Imperatives & Safeguards

1. Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience
   - Two national CI centers operated by DHS – one for physical and one for cyber infrastructure - function in an integrated manner; focal points to share [actionable] information to protect physical and cyber infrastructures
2. Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government
   - Efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators.
3. Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure
   - Support DHS in sharing a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure.

PPD-21 revokes HSPD-7

Homeland Security

Executive Order - Improving Critical Infrastructure Cybersecurity *(2/12/2013)*

Highlights from the Executive Order:

- **Cybersecurity Information Sharing:**
  - Increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities to better protect and defend themselves against cyber threats
  - Enhanced Cybersecurity Services: voluntary information sharing program will provide classified cyber threat and technical information to eligible CI companies and ISPs that offer security services to critical infrastructure.
- **Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.**
  - Working with NIST to develop a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks (includes voluntary consensus standards and industry best practices).
- **Identification of Critical Infrastructure at Greatest Risk**
  - Identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

Consultation from; industry experts, academia, SSAs, regulatory agencies, Federal agencies, etc., to coordinate improvements to the cybersecurity of critical infrastructure.

Homeland Security

DHS Cyber Security Evaluations

CYBER RESILIENCE REVIEW & CYBER SECURITY EVALUATION TOOL

Homeland Security

Resilience through Measurement - 1

A process for identifying and analyzing vulnerabilities is established and maintained

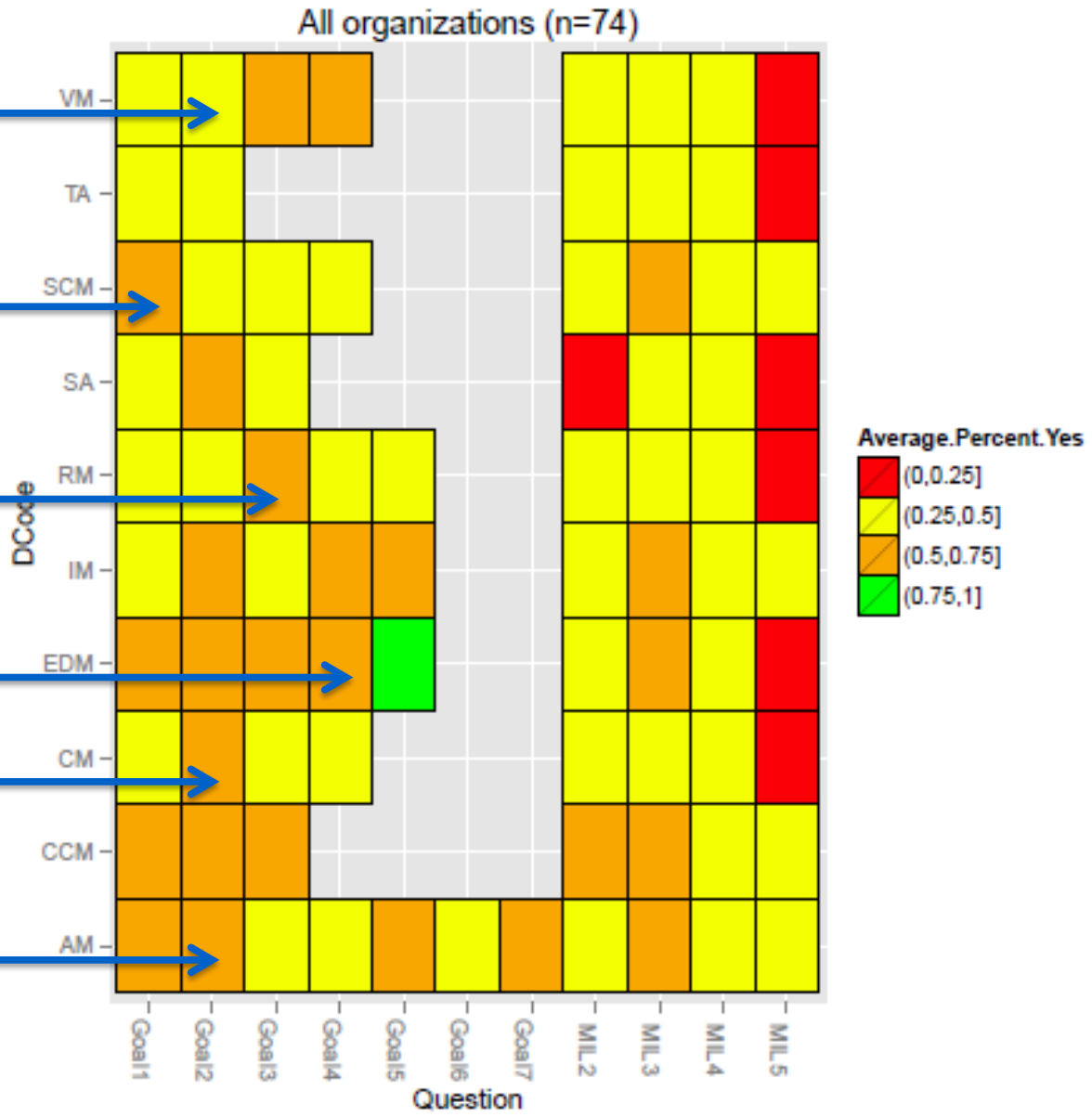
Service continuity plans for high-value services are developed

Risks are identified

Relationships with external entities are formally established and maintained

Controls are implemented

Assets are inventoried, and the authority and responsibility for these assets is established



Homeland Security

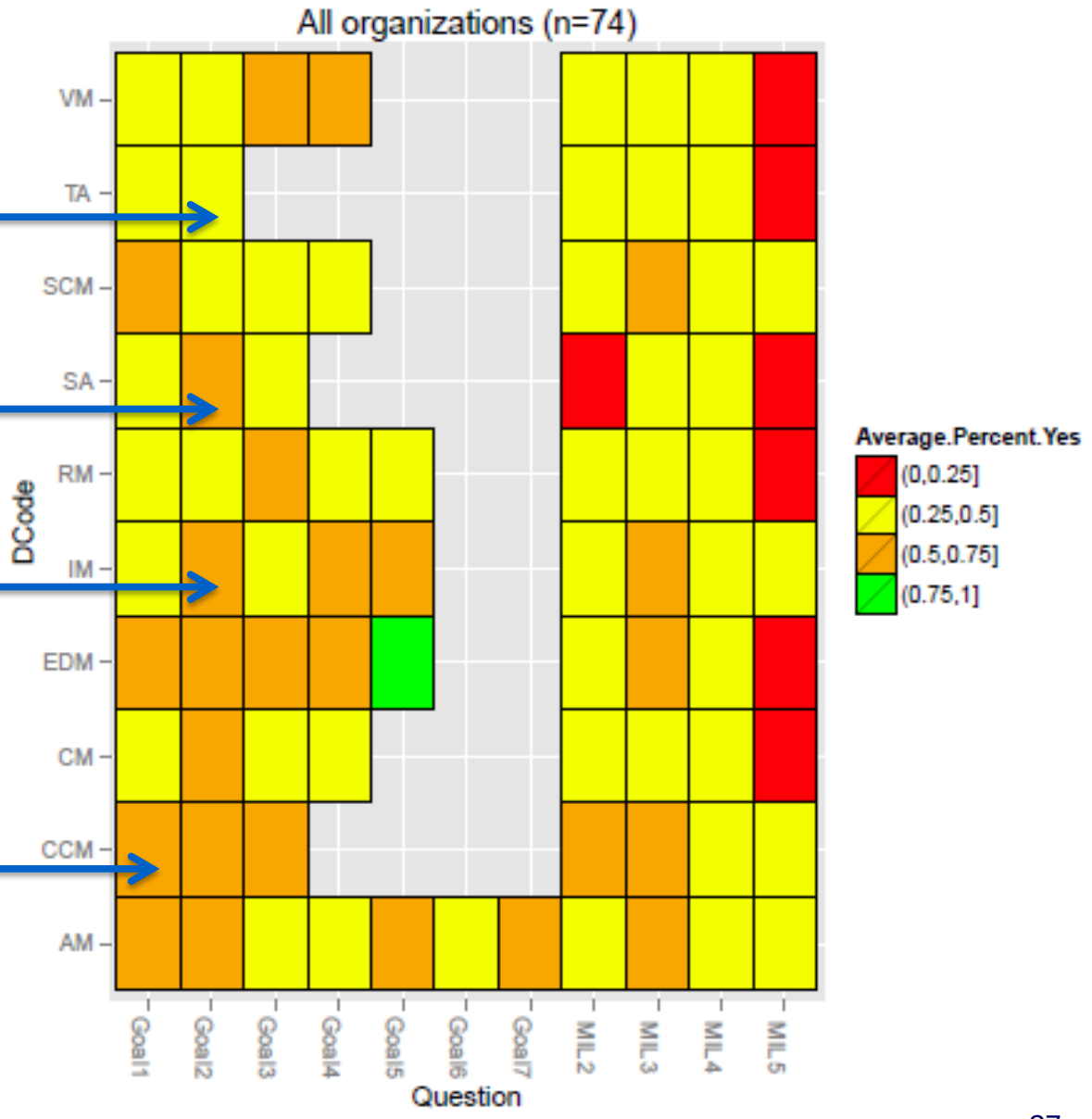
Resilience through Measurement - 2

Awareness and training activities are conducted

The requirements for communicating threat information are established

A process for detecting, reporting, triaging, and analyzing events is established

The life cycle of assets is managed (via change control and management)



Homeland Security

CYBER RESILIENCE REVIEW (CRR)

Homeland Security

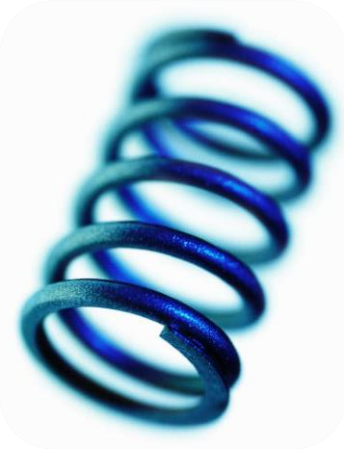
Cyber Resilience Review (CRR)

- Based on the ***CERT® Resilience Management Model (RMM)***, a process improvement model for managing operational resilience
- Development of CRR methodology began in early 2009
- Deployment across all 18 CIKR sectors as well as State, local, tribal, and territorial governments
- **Primary goal:** Evaluate how CIKR providers manage cyber security of significant information services and assets (information, technology, facilities, and personnel)
- **Secondary goal:** Identify opportunities for improvement in cyber security management and reduce operational risks related to cyber security

Homeland Security

Cyber Resilience

- Definition:
  - The ability of an organization to continue vital IT services and information management functions in a less-than-ideal situation while reacting and adapting to stresses



Protect (Security)	Sustain (Continuity)
Perform (Capability)	Repeat (Maturity)

Homeland Security

CRR Domains

- These represent key areas that typically contribute to an organization's cyber resilience— each domain focuses on:
  - **Documentation** in place, and periodically reviewed & updated
  - **Communication** & **notification** to all those who need to know
  - **Execution/Implementation** & **analysis** in a consistent, repeatable manner
  - **Alignment** of goals and practices within & across CRR domains

AM	**Asset Management** *identify, document, and manage assets during their life cycle*	SCM	**Service Continuity Management** *ensure continuity of IT operations in the event of disruptions*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	RISK	**Risk Management** *identify, analyze, and mitigate risks to services and IT assets*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	EXD	**External Dependency Management** *manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge*
IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

Maturity Not Just Capability

- A **MIL (Maturity Indicator Level)** measures ***process institutionalization***, and describes attributes indicative of mature capabilities.

MIL Level 5 – Defined

All practices are performed (MIL-1); planned (MIL-2); managed (MIL-3); measured (MIL-4); and consistent across all internal constituencies who have a vested interest— processes/practices are defined by the organization and tailored by organizational units for their use, and supported by improvement information shared amongst organizational units.

MIL Level 4 – Measured

All practices are performed (MIL-1); planned (MIL-2); managed (MIL-3); and periodically evaluated for effectiveness, monitored & controlled, evaluated against its practice description & plan, and reviewed with higher-level management.

MIL Level 3 – Managed

All practices are performed (MIL-1); planned (MIL-2); and governed by the organization, appropriately staffed/funded, assigned to staff who are responsible/accountable & adequately trained, produces expected work products, placed under appropriate configuration control, and managed for risk.

MIL Level 2 – Planned

All practices are performed (MIL-1); and established, planned, supported by stakeholders, standards and guidelines.

MIL Level 1 – Performed

All practices are performed, and there is sufficient and substantial support for the existence of the practices.

MIL Level 0 – Incomplete

Practices are not being performed, or incompletely performed.

Homeland Security

CRR Report

CYBER RESILIENCE REVIEW REPORT

FOR

SITE NAME

MONTH XX, 2012

UNITED STATES DEPARTMENT OF HOMELAND SECUR

NATIONAL CYBER SECURITY DIVISION

CYBER SECURITY EVALUATION PROGRAM

– CUSTOMER REVIEW COPY –

DOMAIN 1: ASSET MANAGEMENT

The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC:SG2.SP1]	Incomplete
	Option(s) for Consideration	
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Prioritize your organization's critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional Reference:** NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
	Option(s) for Consideration	
Q1	**CERT-RMM Reference:** [ADM:SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. **Additional Reference:** NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	

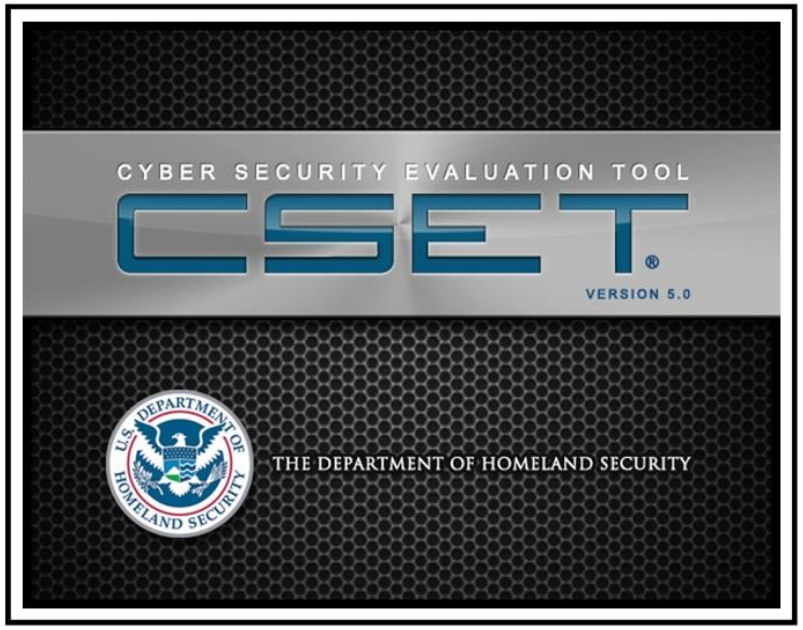
Homeland Security

CYBER SECURITY EVALUATION TOOL (CSET)

Homeland Security

Cyber Security Evaluation Tool (CSET®)

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy



CSET Download:

http:/us-cert.gov/control_systems/csetdownload.html

Homeland Security

CSET® Standards

Requirements Derived from Widely Recognized Standards

NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems Rev 3 and with Appendix I, ICS Controls
TSA Pipeline Security Guidelines	Transportation Security Administration (TSA) Pipeline Security Guidelines, April 2011
NERC Critical Infrastructure Protection (CIP)	Reliability Standards CIP-002 through CIP-009, Revisions 2 and 3
DoD Instruction 8500.2	Information Assurance Implementation, February 6, 2003
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security, June, 2011
NRC Reg. Guide 5.71	Cyber Security Programs for Nuclear Facilities, January 2010
CFATS RBPS 8- Cyber	Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
DHS Catalog of Recommendations	DHS Catalog of Control Systems Security, Recommendations for Standards Developers, Versions 6 and 7

Homeland Security

CSET Main Window

File Windows Help

CSET

INFORMATION | STANDARDS | DIAGRAM | QUESTIONS | ANALYSIS | REPORTS

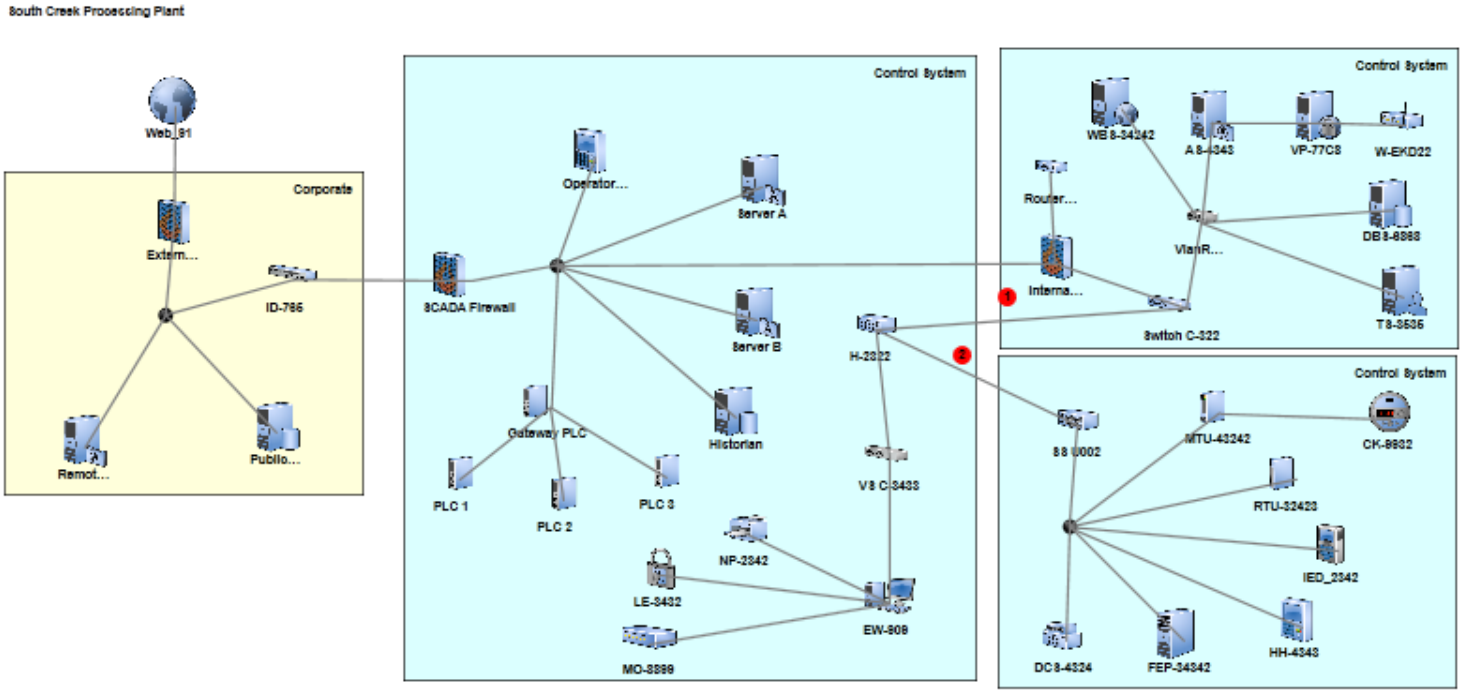
RESOURCE LIBRARY

DIAGRAM SYMBOLS

DOCUMENT LIBRARY

DIAGRAM PROPERTIES

Tools Diagram Drawing Format



STANDARDS PREVIOUS NEXT QUESTIONS

CSET Main Window

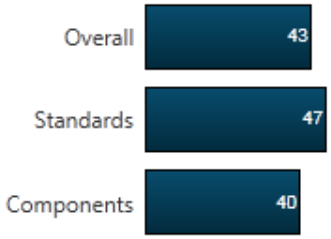
File Windows Help

CSET

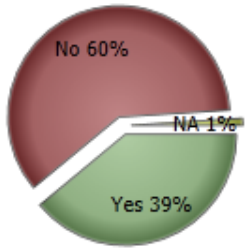
INFORMATION | STANDARDS | DIAGRAM | QUESTIONS | ANALYSIS | REPORTS | RESOURCE LIBRARY

DOCUMENT LIBRARY

Assessment Compliance

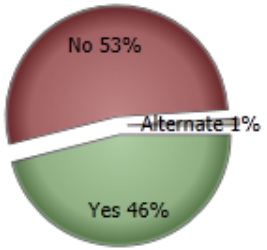


Components Summary Results



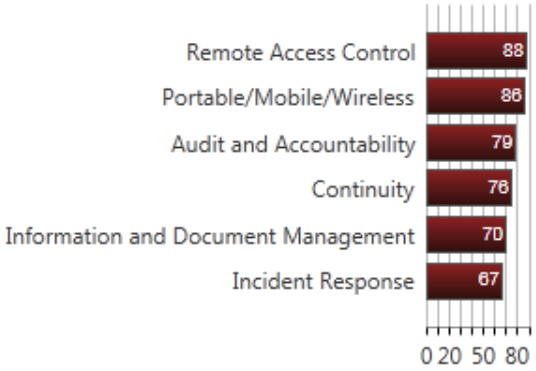
Yes No NA
Alternate Unanswered

Standards Answers Summary

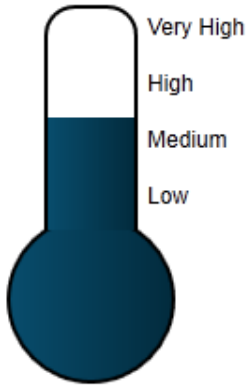


Yes No NA
Alternate Unanswered

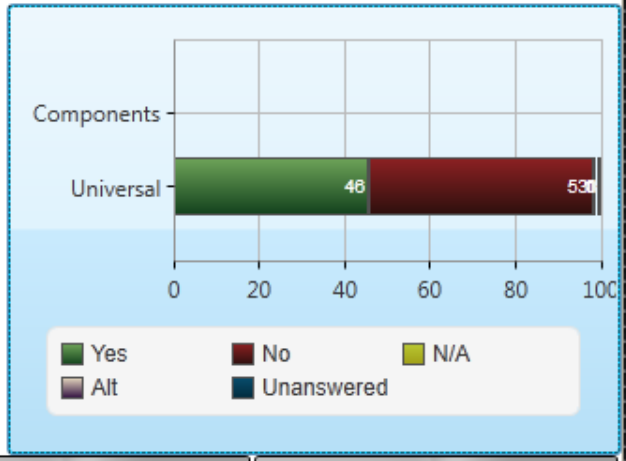
Standards Top Categories of Concern



Security Assurance Level:



Summary of Results by Selected Standards



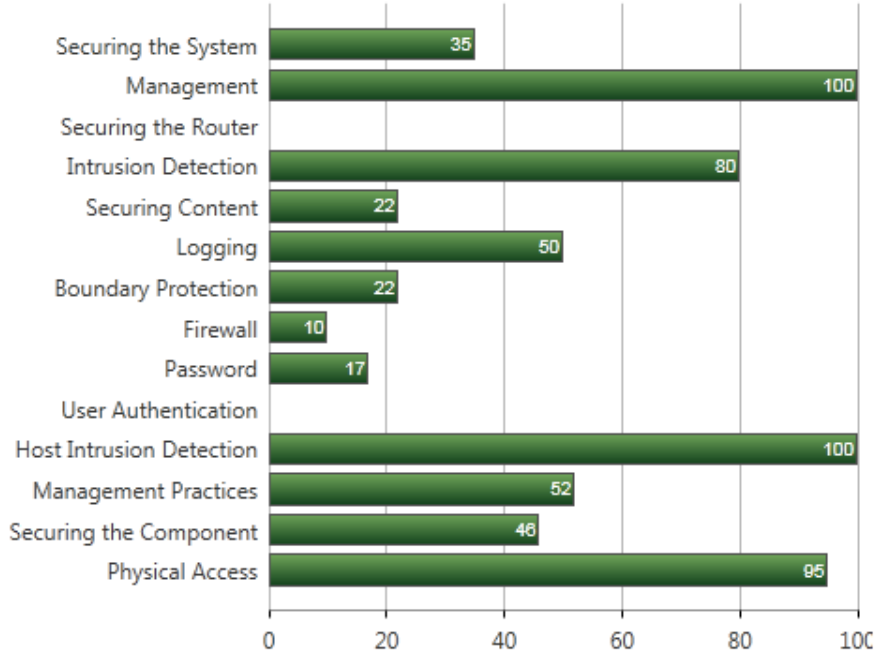
Network Warnings | Top Concerns | Unanswered Questions | Questions With Comments | Questions Marked for Review

QUESTIONS ← PREVIOUS NEXT → REPORTS

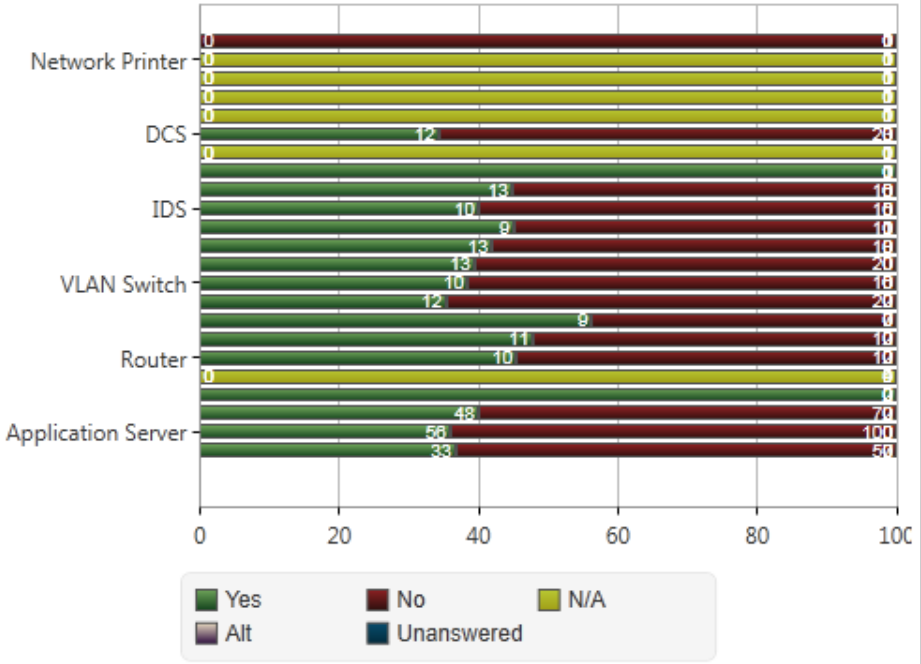
Components Summary

Components Summary

Components by Category



Components by Component Type

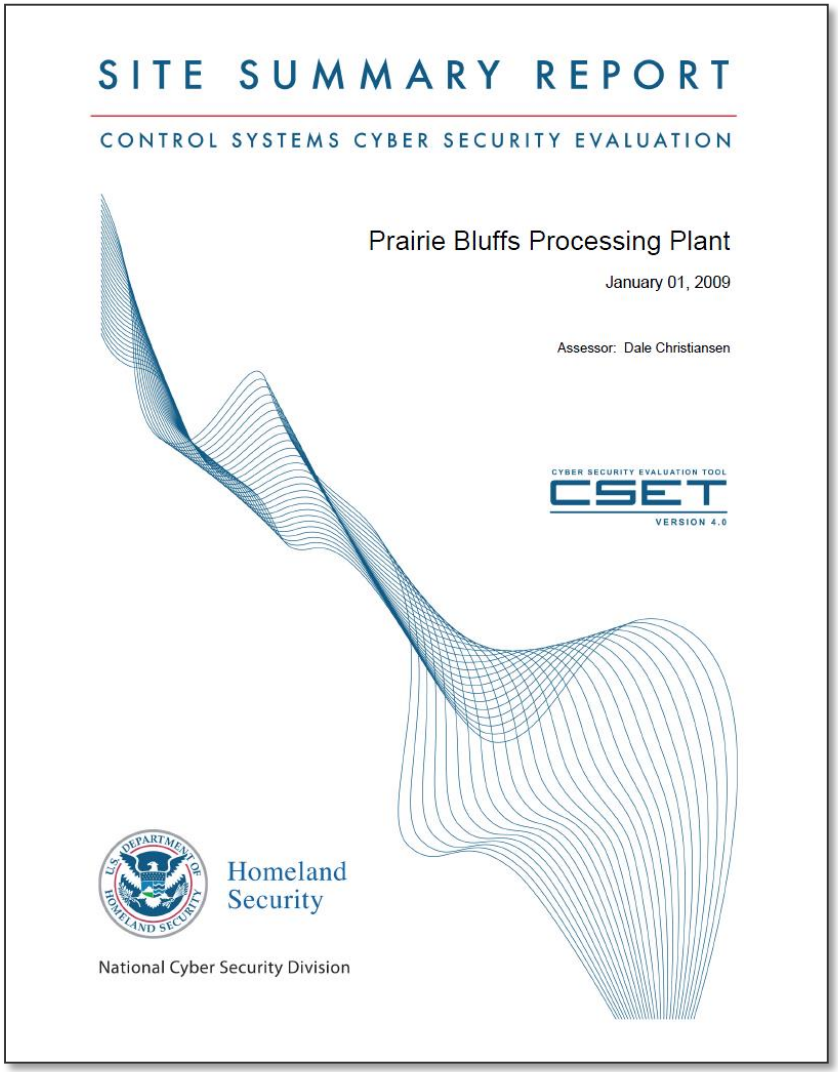


	Yes	Total Questions	Percent
Physical Access	20	21	95
Securing the Component	111	243	46
Management Practices	47	91	52
Host Intrusion Detection	17	17	100
User Authentication	0	16	0
Password	16	92	17
Firewall	4	39	10
Boundary Protection	7	32	22
Logging	21	42	50
Securing Content	11	49	22

Component	# Components	# Questions	Total Questions	Yes	No	N/A	Alt	Unanswe
Firewall	3	30	90	33	57	0	0	33
Applicatio	4	39	156	56	10	0	0	56
Database	3	40	120	48	72	0	0	48
HMI	2	1	2	2	0	0	0	2
PLC	4	1	4	0	0	4	0	4
Router	1	22	22	10	12	0	0	10
VLAN Rou	1	23	23	11	12	0	0	11
Switch	1	16	16	9	7	0	0	9
Serial Swi	1	34	34	12	22	0	0	12
VLAN Swi	1	26	26	10	16	0	0	10

OK

Hard-copy Reports



SITE SUMMARY REPORT

CONTROL SYSTEMS CYBER SECURITY EVALUATION

Prairie Bluffs Processing Plant

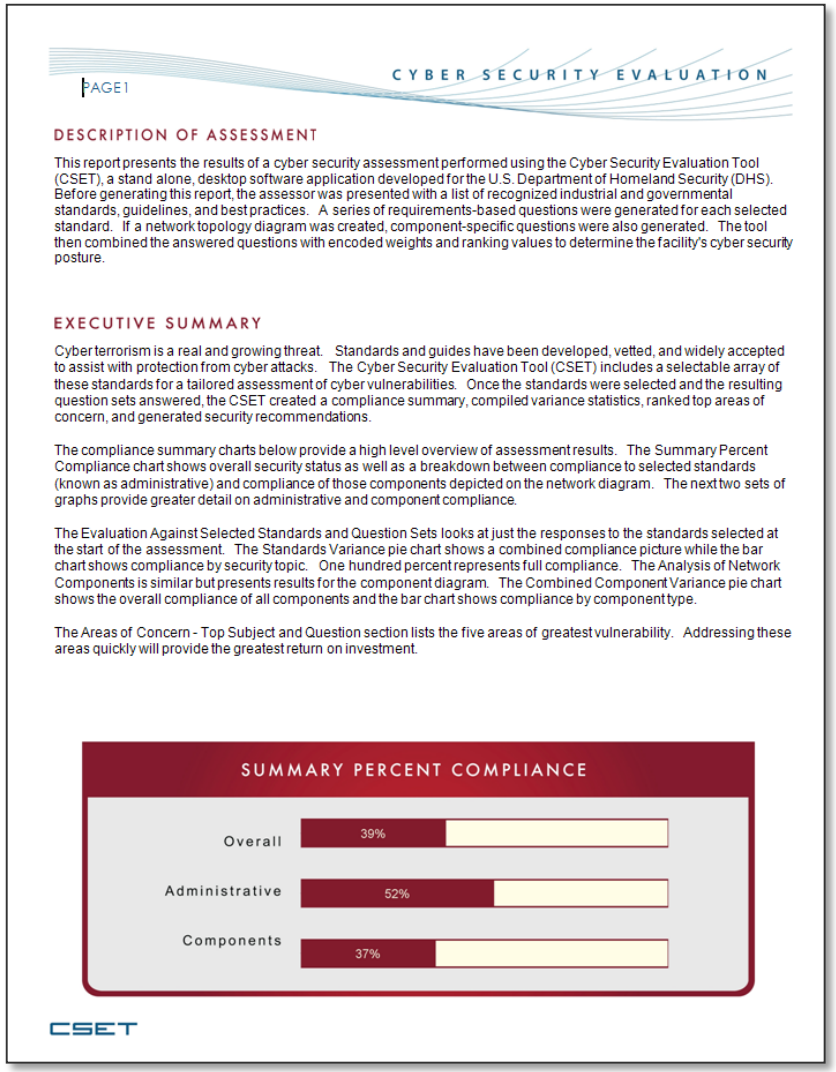
January 01, 2009

Assessor: Dale Christiansen

CYBER SECURITY EVALUATION TOOL
CSET
VERSION 4.0

Homeland Security

National Cyber Security Division



PAGE 1

CYBER SECURITY EVALUATION

DESCRIPTION OF ASSESSMENT

This report presents the results of a cyber security assessment performed using the Cyber Security Evaluation Tool (CSET), a stand alone, desktop software application developed for the U.S. Department of Homeland Security (DHS). Before generating this report, the assessor was presented with a list of recognized industrial and governmental standards, guidelines, and best practices. A series of requirements-based questions were generated for each selected standard. If a network topology diagram was created, component-specific questions were also generated. The tool then combined the answered questions with encoded weights and ranking values to determine the facility's cyber security posture.

EXECUTIVE SUMMARY

Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.

The compliance summary charts below provide a high level overview of assessment results. The Summary Percent Compliance chart shows overall security status as well as a breakdown between compliance to selected standards (known as administrative) and compliance of those components depicted on the network diagram. The next two sets of graphs provide greater detail on administrative and component compliance.

The Evaluation Against Selected Standards and Question Sets looks at just the responses to the standards selected at the start of the assessment. The Standards Variance pie chart shows a combined compliance picture while the bar chart shows compliance by security topic. One hundred percent represents full compliance. The Analysis of Network Components is similar but presents results for the component diagram. The Combined Component Variance pie chart shows the overall compliance of all components and the bar chart shows compliance by component type.

The Areas of Concern - Top Subject and Question section lists the five areas of greatest vulnerability. Addressing these areas quickly will provide the greatest return on investment.

SUMMARY PERCENT COMPLIANCE

Overall 39%

Administrative 52%

Components 37%

CSET

Homeland Security

CSET Resource Library

RESOURCE LIBRARY

Document Tree | Search

- Guidance
- Reports
- Templates
  - Cryptography & Encryption
  - Processes & Procedures
  - Access Control
  - Service Providers
  - Wireless
  - Incidents
  - Security Plans
    - Contingency Plan_IT-HHS Template
    - CyberSec Plan-NRC Template
    - IT Disaster Recovery Plan-FLA Templa
    - InfoSec Plan-AbqSPIN Template
    - InfoSec ISS-Neb Template
    - Sec Approach Plan-HHS Template
    - SecPlan-CoSN Template
    - SecPlan_Major Apps-USG Template
    - SecPlan-LMRs-PSWN Template
    - SecPlan_Network-QIT Template
    - SSP-HHS Template
    - SSP-Mod Impact-NIST Template
    - Lab Policy Template-SANS
  - Nuclear
  - Access control
  - Test & Evaluation
  - Servers
  - Communications
- Standards
- Cyber Security Procurement Language
- Catalog of Recommendations

Resource Library

This library of cyber security standards, reports, and templates are provided for your convenience. Additionally there are several cyber security guides and white papers to assist you in gaining a general background in cyber security, determining priorities, or specific helps. Specific helps include white papers and instructions on securing network components such as a firewall or web server.

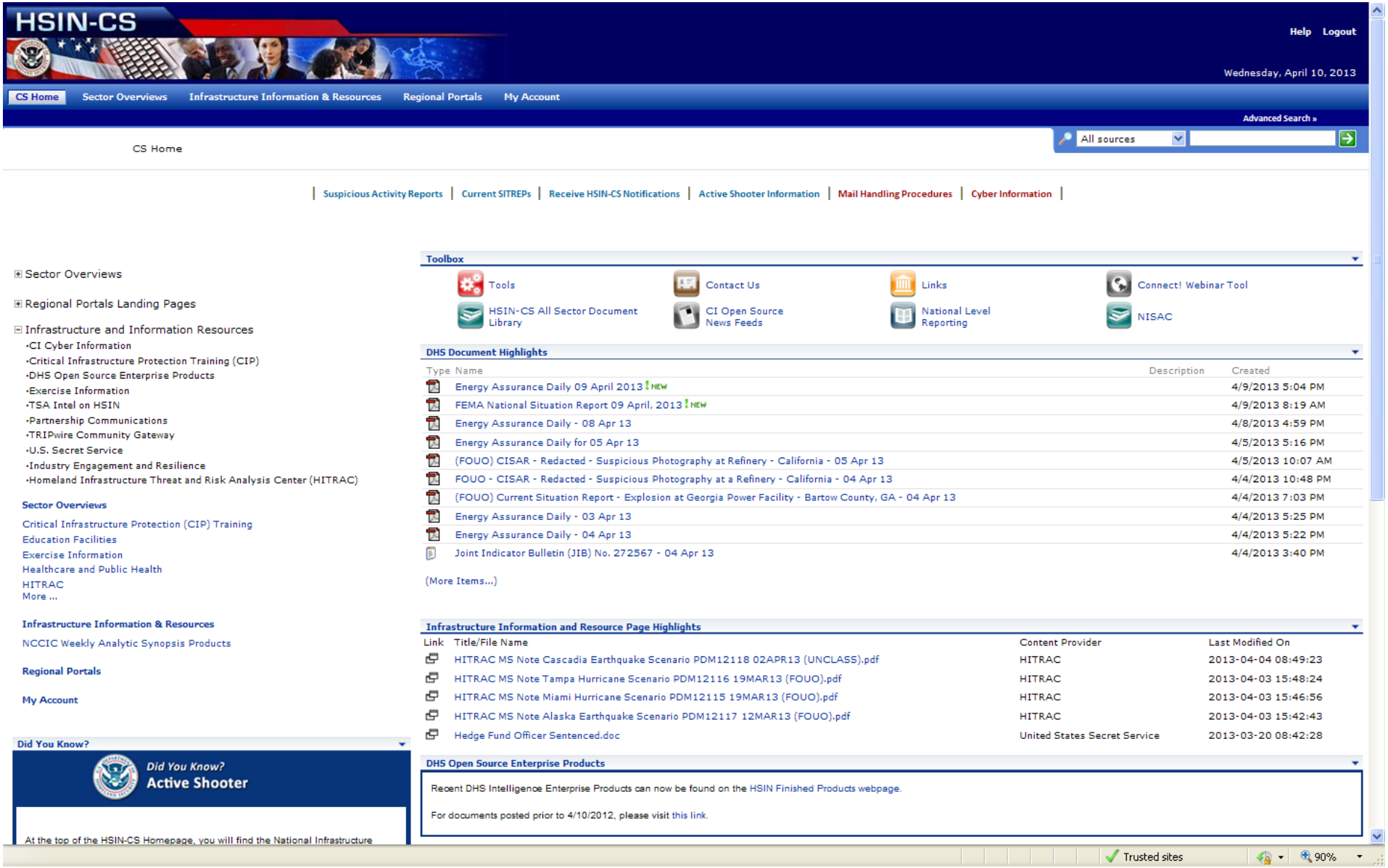
Library documents may be browsed using the “Document Tree” tab on the left side of the screen. Documents are grouped by type and topic. If you are looking for a specific document a keyword or title search may also be performed using the “Search” tab in the left pane. Clicking on a document title link in the left-hand pane displays the document. To save a document to your local hard drive click the export button.

Don’t Forget about HSIN

HOMELAND SECURITY INFORMATION NETWORK (HSIN)

Homeland Security

Homeland Security Information Network



HSIN Resource Library and Reports

	CyberCom MMA 12-032	2/19/2013 9:03 AM	Information Technology	Alerts and Advisories	Network Security and Defense; Malicious Tactics, Techniques, and Procedures; Malware Analysis
	ICS-ALERT - Offline Brute-Force Password Tool Targeting Siemens S7	1/24/2013 11:13 AM	Information Technology	Alerts and Advisories	Malicious Tactics, Techniques, and Procedures
	Symantec - Ransomware-A Growing Menace	11/9/2012 1:08 PM	All Sectors	Alerts and Advisories	End User Security
	ICS-CERT - ALERT 12-097-02A - 3S Software Codesys Improper Access Control	10/29/2012 10:26 AM	All Sectors	Alerts and Advisories	Malicious Tactics, Techniques, and Procedures
	ICS-CERT - ALERT 12-046-01 - Increaasing Threat to Industrial Control Systems	10/29/2012 10:25 AM	All Sectors	Alerts and Advisories	Malicious Tactics, Techniques, and Procedures
	Panda Security - Main computer security threats - Trojans	10/26/2012 12:32 PM	All Sectors	Alerts and Advisories	Intelligence and National Security
	Internet Crime Complaint Center - Fraud Alert - Financial Institution Employee Credentials Targeted	9/18/2012 11:38 AM	Banking and Finance	Alerts and Advisories	Malicious Tactics, Techniques, and Procedures
	DHS - Criminals and Hacktivists May Use 2012 Summer Olympics as Platform for Cyberattacks	5/24/2012 9:55 AM	All Sectors	Alerts and Advisories	Malicious Tactics, Techniques, and Procedures
	DHS - Attack Surface - Healthcare and Public Health Sector	5/16/2012 5:11 PM	Healthcare and Public Health	Alerts and Advisories	Network Security and Defense
	Fraud Advisory for Businesses - Corporate Account Take Over	4/6/2012 3:50 PM	Banking and Finance; All Sectors	Alerts and Advisories	Intelligence and National Security
	Fraud Advisory for Consumers - Involvement in Criminal Activity through Work from Home Scams	4/6/2012 3:49 PM	All Sectors	Alerts and Advisories	Intelligence and National Security

Homeland Security

Resilience Starts with Good Hygiene

Review Layers of Defense:

- Human: → **Policies, Procedures, Training**
- Applications: → **Control Systems, Databases**
- Operating Systems: → **Patch Management, Setup**
- Networks: → **Firewalls, Detection Systems**
- Physical: → **Guards, Gates, Surveillance, Lighting**

- Review Critical Assets and Important Services
- Identify Security and Business Continuity Requirements
- Map Requirements to Security Standards
- Apply Risk-Based Solutions
- Monitor, Monitor, Monitor… (Lather, Rinse, Repeat…)
- Work with your community-of-interest and other resources

Homeland Security

DHS Cyber Resources - Reminder

- **National Cybersecurity and Communications Integration Center (NCCIC)**
  - Serves as a national center for reporting and mitigating communications and cybersecurity incidents. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
  - Provides:
    - 24x7 real-time threat analysis and incident reporting capabilities, at 1-888-282-0870
    - Malware Submission Process:
      - Please send all submissions to: submit@malware.us-cert.gov
      - Must be provided in password-protected zip files using password "infected"
      - Web-submission: https://malware.us-cert.gov
    - ICS-CERT Training: http://ics-cert.us-cert.gov/cscalendar.html
- **Cyber Security Evaluations Program (cse@hq.dhs.gov)**
  - Provides no-cost, voluntary cyber security evaluations and assessments, including:
    - Cyber Resilience Review (CRR)
      - One-day, facilitated evaluation focused on critical IT services and the security management process
    - Cyber Security Evaluation Tool (CSET)
      - Stand-alone software application, used as a self-assessment against recognized standards and a tool for creating a baseline of cybersecurity practices
      - Downloadable at: http:/us-cert.gov/control_systems/csetdownload.html

Homeland Security

DHS Contact Information	
Bradford Willke Cyber Security Advisor, Mid-Atlantic Region	bradford.willke@hq.dhs.gov
General Inquiries	
cyberadvisor@hq.dhs.gov	

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications